EXPLANATORY MEMORANDUM

1. INTRODUCTION

Citizens increasingly perform daily activities and transactions using electronic communications networks and services. These communications generate 'traffic data' or 'location data' which include for example details about the location of the caller, the number called, the time and duration of the call.

Directive 2002/58/EC on Privacy and Electronic Communications harmonises through its Articles 6 and 9 the personal data protection rules which are applicable to the processing of traffic and location data generated by the use of electronic communications services. Such data must be erased or made anonymous when no longer needed for the purpose of the transmission, except for the data necessary for billing or interconnection payments; subject to consent, certain data may also be processed for marketing purposes and the provision of value added services.

When combined with data enabling the identification of the subscriber or user of the service, the availability of such traffic data is important for purposes related to law enforcement and security, such as the prevention, investigation, detection and prosecution of crime and terrorism. This is recognised in Article 15 (1) of Directive 2002/58, which stipulates that Member States may provide for restrictions of the scope of (amongst others) Articles 6 and 9 mentioned above, when such restrictions constitute a necessary, appropriate and proportionate measure within a democratic society to safeguard national security, defence, public security and the prevention, investigation, detection and prosecution of criminal offences. As a consequence, these purposes can be invoked to justify the storage and processing of traffic and location data other than in accordance with Articles 6 and 9.

It has now become urgent to adopt harmonised provisions at EU level on this subject. A certain number of Member States have adopted, or plan to adopt, national measures requiring some or all operators to retain given types of data so that they can be used for the purposes identified above when necessary. Differences in the legal, regulatory, and technical provisions in Member States concerning the retention of traffic data present obstacles to the Internal Market for electronic communications as service providers are faced with different requirements regarding the types of data to be retained as well as the conditions of retention. These provisions should therefore be further harmonised in accordance with Article 14 of the EC-Treaty.

The necessity to have rules at EU level that guarantee the availability of traffic data for anti-terrorism purposes across the 25 Member States was also confirmed by the European Council in its Declaration on combating terrorism of 25 March 2004. Following the Madrid terrorist bombings, the European Council instructed the Council to examine 'proposals for establishing rules on the retention of communications traffic data by service providers'. The Declaration also stated that priority should be given to these with a view to adoption in 2005. The priority attached to adopting an appropriate legal instrument on this subject was recently confirmed in the Conclusions of the European Council of 16 and 17 June, as well as at the special JHA Council meeting of 13 July.

Whilst the desirability of establishing rules on this issue from a public security perspective is therefore clearly established, it is important to find an appropriate balance between different

kinds of interests, sometimes diverging: law enforcement needs, human rights and competition aspects. An approach needs to be found which takes these different interests into consideration.

In terms of protecting risks to the private life of citizens, this can be achieved firstly through clearly establishing the purpose for which data which are retained can be used, secondly through limiting the categories of data which need to be retained, and thirdly through limiting the period of retention time. Another important safeguard is that this Directive is not applicable to the content of communications – this would amount to interception of telecommunications, which falls outside the scope of this legal instrument.

Another point worth considering within this context is that the personal data retained by the service and network providers under the provisions of this Directive are covered by the general and specific data protection provisions established under Directives 95/46/EC and 2002/58/EC – which means in practice that additional provisions on general data protection principles and data security are not necessary. It also means that the processing of such data will be under the full supervisory powers of the data protection authorities established in all Member States.

As a final protective element, the Directive foresees an active involvement of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC in the evaluation process of the Directive.

These guarantees will aid in ensuring that the threat to the private life of citizens of this measure will be very limited, and that the data will be used by a limited number of competent authorities, and for well-established, legitimate purposes. At the same time, it should be recognised that the rules establishing the authorities competent to have access to the data, and the subsequent use of such data, are to a large extent issues which belong to the competence of the Member States. They therefore fall outside the authority of the Community legislator, and can only be regulated at the EU level insofar as the Treaty on European Union provides for a legal basis for this. The same is true for cooperation between competent authorities across borders - this is not addressed by the present instrument, since approximation of national provisions governing such cooperation must be pursued under Title VI of the Treaty on European Union.

In order to ensure that the Directive stays up-to-date within the rapidly changing technical environment of electronic communications, it provides for two additional elements. Firstly, a Comitology mechanism is foreseen to allow for quick amendments to the details of the data which need to be retained. Secondly, the Directive sets up an advisory Platform with representatives of law enforcement, the electronic communications industry and data protection authorities, which will provide for opportunities to work together on this difficult, but important issue in a public-private partnership approach. The Platform will be consulted whenever the details of the list of data to be retained are to be amended.

2. AIMS AND OBJECTIVES

The proposed Directive is intended to harmonise obligations for providers of publicly available electronic communications services or a public communications network to retain certain data for the purpose of the prevention, investigation, detection and prosecution of criminal offences.

As a consequence the provisions of the first paragraph of Article 15 of Directive 2002/58/EC, relating to the prevention, investigation, detection and prosecution of criminal offences, need to be amended as the measures related to them are harmonised with this Directive.

The Directive also confirms that it applies not only to data related to natural persons, but also to data related to legal persons. There is no legitimate reason why communications emanating from a legal person should not be covered by this Directive – there are certainly cases where this information, even if it does not yet provide a link to the actual person involved in the communication, is a useful starting point for further inquiries and investigation by the competent authorities. It should not be possible for suspects of crime and terrorism to 'hide behind' a corporate front, and thus escape the application of the data retention obligations.

It has been argued that an obligation to retain traffic data of the electronic communications of all citizens is a disproportionate measure, since it targets not only suspects of crime and terrorism. This argument is usually accompanied by a reasoning which states that measures to preserve data related to only those suspects would be an equally adequate measure. Whilst it is certainly true that measures obliging network and service providers to preserve data on specific suspects is necessary, both for preventive and investigative purposes, those measures can only cover the needs of law enforcement partially, since this only relates to the communications of those persons as of the moment they have become suspects. Without a general obligation of data retention, it is not guaranteed that law enforcement can investigate communications which took place before the crime or act of terrorism was actually committed. This would then depend on the availability of data which was retained coincidentally, or on prior knowledge by law enforcement of the identity of a suspect before a crime is actually committed. However, electronic communications which took place before the actual criminal event took place will provide valuable clues and evidence as to the preparation of offences, and the other persons who were involved in that preparation. The conclusion drawn from this must be that a general data retention obligation is an indispensable element for the prevention and investigation of crime, in addition to the possibilities offered by data preservation schemes, which can only focus on specific persons identified beforehand by the law enforcement authorities.

The proposed Directive harmonises the following elements: (a) the types of data to be retained, (b) the periods of time during which the data should be retained (c) the purposes for which the data may be supplied to the competent authorities. It also provides for an obligation on the service providers to retain the data in such a way that they can co-operate with the competent authorities without undue delay, whilst leaving it to the Member States to determine which authorities are competent under national legislation. Finally, the Directive also provides for the principle of reimbursement of the additional costs incurred by the network and service providers to comply with the obligations imposed on them as a consequence of this Directive. This is an essential element to ensure that there will be no market distortion through the application of different national cost reimbursement schemes.

3. DESCRIPTION OF ARTICLES

Articles 1 and 2: Scope and Aim and Definitions

The provisions on the scope and aim of the Directive are covered in the general part of this explanatory memorandum. With respect to the definitions it should be noted that this Directive uses to a large extent the definitions already established in the general legal

framework regulating the electronic communications sector. This provides the benefit of a consistent approach, and makes it possible to limit the introduction of new definitions.

Article 3: Obligation to retain data

This provision is the core element of the proposal and is largely self-explanatory. Member States must adopt measures to ensure that data which are processed by providers of publicly available electronic communication services or a public communications network within their jurisdictions are retained in accordance with the provisions of this Directive. The definitions ensure that both network and service providers are covered by this provision.

The second paragraph guarantees that the relevant information can only be provided for the purposes of prevention, investigation, detection and prosecution of criminal offences. This wording is taken directly from Article 15 (1) of Directive 2002/58/EC.

Given the amendment proposed to Article 15 of Directive 2002/58/EC in Article 9 of the current proposal, it is necessary to specify that the measures foreseen under the new Directive provide for a restriction of the scope of the rights laid down in Articles 5, 6 and 9 of Directive 2002/58/EC.

Article 4: Categories of information to be retained

Rather than providing a detailed technical description of the various types of data to be retained, the Directive itself lists the categories of information that electronic service providers should be able to make available to the competent authorities. Such a 'result-oriented' list provides a certain degree of flexibility to the Member States in deciding what obligations will need to be met and to the operators on how to meet these obligations. The further detail of the types of data to be retained under these categories is included in the Annex to the Directive, which can be amended quickly using the Comitology approach. In order to assist Member States in the implementation of the Directive, an advisory Platform will be created consisting of representatives of the Member states and their law enforcement authorities, data protection authorities and industry representatives. Both this Platform and the Article 29 Working Party will be involved in any amendments to the list of types of data to be retained.

Article 5: Retention periods

With respect to the periods of time for retention, as indicated before, an appropriate balance must be struck between the different interests at stake. The fact that there is no way of predicting with any certainty what communication data is going to provide the essential element in preventing a terrorist attack or finding the perpetrator of a crime, and how old that communication data is going to be once the competent authorities discover that they need it, would point in the direction of longer retention periods. The other interests identified before - a limited invasion of privacy, and a limited impact on the competitiveness of the electronic communications industry - would dictate shorter periods. At the current time, where in the Member States the periods of obligatory data retention vary between 6 months and 4 years, a period of one year for traditional fixed and mobile electronic communication services and of 6 months for electronic communications using the Internet Protocol (IP-based communications) is seen as a proportionate solution which will accommodate all interests involved. This is also based on the Impact Assessment prepared by the Commission. The use of the phrase "solely the Internet Protocol" in both paragraphs of the Article indicates that data related to electronic

communications which start from an internet base, but connect to a traditional fixed or mobile number should be retained for one year.

Article 6: Storage requirements for retained data

This article ensures that the data must be retained in such a manner as to ensure that requests for transfer of the data to the competent authorities can be dealt with in a speedy and effective manner. This implies also that it must be technically feasible to provide information on the main categories of data specified under Article 4 quickly and easily. It also provides for an obligation to submit additional information to the competent authorities – e.g. on the details of the retention scheme utilised by the electronic communications and network service providers - in order to ensure that the co-operation with the competent authorities will proceed smoothly.

Article 7: Statistics

Today no verifiable statistics exist at the European level on the usage of traffic data. This article provides for the obligation of services and network providers to keep statistics on the number of cases they have actually supplied information to the competent authorities, including information on how old the data was when it was supplied to those authorities, and to provide such information to the Commission on a yearly basis. For reasons of proportionality and protection of privacy, it also makes explicit that this information should not contain the personal data of the persons regarding whom information was requested by the competent authorities. This information, once aggregated, will provide the factual information necessary to evaluate the effectiveness of the Directive.

Article 8: Costs

As indicated above, the obligation to retain data in such a way that the relevant information can be made available to the competent authorities upon request may lead to additional costs for the service and network providers. It is reasonable for governments to contribute to meeting the costs incurred as a consequence of the implementation of this Directive. The Article stipulates that this should be limited to demonstrated additional costs which the providers have had to incur in order to comply with the obligations imposed on them as a consequence of this Directive.

Article 9: Platform for Law Enforcement, Electronic Communications and Data Protection

As indicated in the introduction of the Explanatory Memorandum, this Article sets up a formal advisory body, bringing together representatives form law enforcement, the electronic communications industry and European data protection authorities. Practice in some Member States has shown that a thorough discussion between these parties is conducive to finding workable solutions in this difficult area. This is particularly important given the ever-changing environment within which this Directive finds its application.

Article 10: Amendment of Directive 2002/58/EC

As indicated in the general part of this explanatory memorandum, Article 15 (1) of Directive 2002/58/EC needs to be amended in order to ensure that the purpose of harmonisation of the Member States' provisions in this area is actually achieved. This is done through the addition of a new paragraph 2, which clarifies that as far as data retention for the purpose of

prevention, investigation, detection and prosecution of criminal offences is concerned, Member States may no longer make use of the possibility of restricting the scope of certain rights provided for under the first paragraph of Article 15.

Article 11: Evaluation

Given the fact that the current Directive deals with a topic which is closely linked to technological developments, and is likely to have an impact on both law enforcement practices and the electronic communications market, a thorough evaluation of its implementation will assist in identifying whether the Directive has achieved its purpose, and whether any adaptations are necessary. To this end, the evaluation clause contained in Article 10 provides for an obligation on the Commission to evaluate the implementation of the Directive and to inform the European Parliament and the Council of the results. As indicated above, the statistical information gathered under Article 7 should provide a substantial part of the factual information required for that evaluation. The evaluation should also look at the data protection aspects of the implementation of the Directive, which is why the Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC will be consulted during the evaluation process. Also, the Platform set up under Article 9 will be involved in the evaluation exercise. As a result of the evaluation the Commission will consider the need to propose the necessary amendments to the current directive.

Articles 12, 13 and 14 Final Provisions

These articles are the standard closing provisions of a Directive, and provide for the deadline of transposing the Directive into national law, the entry into force of the Directive and the fact that the Directive is addressed to the Member States.

4. LEGAL BASIS

The legal basis is Article 95 of the EC-Treaty. As indicated before, differences in the legal, regulatory, and technical provisions in Member States concerning the retention of certain data, as well as cost compensation schemes, present obstacles to the Internal Market for electronic communications as service providers are faced with different requirements regarding the types of data to be retained as well as the conditions and the duration of retention. These provisions should therefore be further harmonised in accordance with Article 14 of the EC-Treaty.

The choice for an EC-Treaty legal basis is also related to the fact that both Directives 95/46 and 2002/58 already provide for rules on how these types of data should be processed – with Article 15 (1) making an explicit reference to provisions on the storage of traffic data. This implies that further legislative action in this area should also be based on a first pillar legal basis, as opposed to a third pillar legal basis. This choice is also in line with the wording of Article 47 of the Treaty on European Union (TEU), which stipulates the relationship between the EC Treaties and the TEU. Under this Article 47, nothing in the EU Treaty shall affect the Treaties establishing the European Communities or the subsequent Treaties and Acts modifying or supplementing them.

Since the objectives of the proposed action cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale and effects of the action, be better achieved at Community level, the Community may adopt measures in accordance with the principle of

subsidiarity as set out in Article 5 of the EC-Treaty. In accordance with the principle of proportionality, as set out in this Article, this Directive does not go beyond what is necessary for those objectives.

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the retention of data processed in connection with the provision of public electronic communication services

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 95 thereof,

Having regard to the proposal from the Commission[1],

Having regard to the opinion of the European Parliament[2],

Having regard to the opinion of the European Economic and Social Committee[3],

Having regard to the opinion of the Committee of the Regions[4],

Whereas:

(1) Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data[5] requires Member States to ensure the rights and freedoms of natural persons with regard to the processing of personal data, and in particular their right to privacy, in order to ensure the free flow of personal data in the Community;

(2) Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector[6] translates the principles set out in Directive 95/46/EC into specific rules for the electronic communications sector;

(3) Articles 5, 6 and 9 of Directive 2002/58/EC define the rules applicable to the processing of personal data by network and service providers of traffic and location data generated by using electronic communications services. Such data must be erased or made anonymous when no longer needed for the purpose of the transmission, except for the data necessary for billing or interconnection payments; subject to consent, certain data may also be processed for marketing purposes and the provision of value added services;

---

1 OJ C [...], [...], p. [...].
2 OJ C [...], [...], p. [...].
3 OJ C [...], [...], p. [...].
4 OJ C [...], [...], p. [...].
5 OJ L 281, 23.11.1995, p. 31.
6 OJ L 201, 30.7.2002, p. 37.

(4) Article 15 (1) of Directive 2002/58/EC sets out the conditions under which Member States may restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1)(2)(3) and (4), and Article 9 of the Directive; any such derogations need to be necessary, appropriate and proportionate within a democratic society for specific public order purposes, i.e. to safeguard national security (i.e. State security) defence, public security or the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communications systems;

(5) Many Member States have adopted legislation providing for the retention of data by service providers for the prevention, detection, investigation and prosecution of crime and criminal offences; the provisions of the various national legislations vary considerably;

(6) The legal and technical differences between national provisions concerning the retention of data for the purpose of prevention, investigation, detection and prosecution of criminal offences present obstacles to the internal market for electronic communications; service providers are faced with different requirements regarding the types of traffic data to be retained as well as the conditions and the periods of retention;

(7) The Conclusions of the JHA Council of 20 September 2001 call for ensuring that law enforcement authorities are able to investigate criminal acts which involve the use of electronic communications and to take legal measures against perpetrators of these crimes, while striking a balance between the protection of personal data and the needs of law enforcement authorities to gain access to data for criminal investigation purposes;

(8) The Conclusions of the JHA Council of 19 December 2002 underline that, because of the significant growth of the possibilities of electronic communications, data relating to the use of electronic communications is particularly important and therefore a valuable tool in the prevention, investigation, detection and prosecution of crime and criminal offences, in particular against organised crime;

(9) The Declaration on combating Terrorism adopted by the European Council on 25 March 2004 instructed the Council to examine measures for establishing rules on the retention of communications traffic data by service providers with a view for adoption by June 2005;

(10) The declaration adopted by the special informal Council of 13 July 2005 reinforces the need to adopt measures related to the retention of electronic communications traffic data as soon as possible;

(11) It is essential to ensure that data which are processed by electronic communication providers when offering public electronic communication services are retained for the prevention, investigation, detection, and prosecution of criminal offences;

(12) The elaboration of categories of information to be retained and the applicable retention periods must reflect an appropriate balance between the benefits for the prevention, detection, investigation and prosecution of crime and terrorism and the level of invasion of privacy they will incur;

(13) It should be recalled that Directive 95/46/EC [7], including Chapter III on judicial remedies, liabilities and sanctions, as well as Directive 2002/58/EC [8] are fully applicable to the data retained in accordance with this Directive;

(14) Since the measures necessary for the implementation of this Directive are measures of general scope within the meaning of Article 2 of Council Decision 1999/468/EC of 28 June 1999[9], laying down the procedures for the exercise of implementing powers conferred on the Commission, they should be adopted by use of the regulatory procedure provided for in Article 5 of that Decision;

(15) This Directive respects the fundamental rights and observes the principles recognised, in particular, by the Charter of Fundamental Rights of the European Union;

HAVE ADOPTED THIS DIRECTIVE:

Article 1
Scope and aim

1. This Directive aims to harmonise the provisions of the Member States on obligations for the providers of publicly available electronic communications services or a public communications network with respect to the processing and retention of traffic and location data of both private and legal persons, as well as the related data necessary to identify the user, in order to ensure that the data is available for the purpose of the prevention, investigation, detection and prosecution of criminal offences.

2. This Directive is not applicable to the content of electronic communications, including information consulted using an electronic communications network.

3. All measures in this Directive shall be in accordance with the general principles of Community Law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.

Article 2
Definitions

1. Unless otherwise provided, the definitions in Directive 95/46/EC, in Directive 2002/21/EC [10], as well as in Directive 2002/58/EC shall apply.

2. For the purpose of this Directive, 'data' means traffic data and location data, as well as the related data necessary to identify the subscriber or user.

---

7 OJ L 281, 23.11.1995, p.31
8 OJ L 201, 30.7.2002, p.37.
9 OJ L 184, 17.7.1999, p. 23.
10 OJ L 108, 24.4.2002, p.33

Article 3
Obligation to retain data

1. Member States shall adopt measures to ensure that data which are generated or processed by providers of publicly available electronic communications services or a public communications network within their jurisdiction in the process of supplying communication services are retained in accordance with the provisions of this Directive, notwithstanding the provisions of Articles 5, 6 and 9 of Directive 2002/58/EC.

2. Member States shall adopt measures to ensure that data retained in accordance with this Directive shall only be provided to the competent national authorities in specific cases and in accordance with national legislation, for the purpose of the prevention, investigation, detection and prosecution of criminal offences.

Article 4
Categories of data to be retained

1. Member States shall ensure that the following categories of data are retained under this Directive:

   a) data necessary to trace and identify the source of a communication;

   b) data necessary to trace and identify the destination of a communication;

   c) data necessary to identify the date, time and duration of a communication;

   d) data necessary to identify the type of communication;

   e) data necessary to identify the communication device or what purports to be the communication device;

   f) data necessary to identify the location of mobile communication equipment.

2. The categories of data referred to in paragraph 1 are further specified in the Annex to this Directive. The Commission will be responsible for revising this Annex on a regular basis as necessary in accordance with the procedure provided for under paragraph 5.

3. The Commission shall be assisted in its task under paragraph 2 by a Committee, composed of representatives of the Member States and chaired by the representative of the Commission.

4. The Commission shall ensure that the Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC, as well as the Platform set up under Article 9 of this Directive are consulted during the revision of the Annex referred to in paragraph 2.

5. Where reference is made to this paragraph, the regulatory procedure laid down in Article 5 of Decision 1999/468/EC shall apply, in compliance with Article 7 (3) and Article 8 thereof.

6. The period provided for in Article 5(6) of Decision 1999/468/EC shall be three months.

Article 5
Periods of retention

1. Member States shall ensure that the categories of data referred to in article 4 are retained for a period of one year, with the exception of data related to electronic communications taking place using solely the Internet Protocol.

2. Member States shall equally ensure that within the categories of data referred to in article 4, those data which relate to electronic communications taking place using solely the Internet Protocol are retained for a period of 6 months.

Article 6
Storage requirements for retained data

Member States shall ensure that the data are retained in accordance with the provisions of this Directive in such a way that the data retained and any other necessary information related to such data can be transmitted upon request to the competent authorities without undue delay.

Article 7
Statistics

Member States shall ensure that providers of publicly available electronic communications services or a public communications network provide statistics to the European Commission on a yearly basis on the cases in which they have provided information to the competent authorities in accordance with national law implementing this Directive, including statistics on the time elapsed between the request and the date when the data have been retained, as well as on cases where requests could not be met. Such statistics shall not contain personal data.

Article 8
Costs

Member States shall ensure that service and network providers offering public electronic communication services will receive an appropriate compensation for demonstrated additional costs they have incurred in order to comply with obligations imposed on them as a consequence of this Directive.

Article 9
Platform for Law Enforcement, Electronic Communications and Data Protection

1. A Platform for Law Enforcement, Electronic Communications and Data Protection, hereinafter referred to as the Platform, will be set up by the Commission. It shall have advisory status and act independently.

2. The Platform shall be composed of representatives of the law enforcement authorities of the Member States and of European law enforcement bodies or organisations, representatives of the European associations of the electronic communications industry, representatives of European data protection authorities or advisory groups, in particular representatives from the Working Party on the protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC, and a representative of the Commission. Each member of the platform shall be designated by the institution, authority, organisation or body which he represents.

3. The Platform shall elect its chairman. The chairman's term of office shall be two years. His appointment shall be renewable.

4. The Platform's secretariat shall be provided by the Commission.

5. The Platform shall adopt it own rules of procedure.

6. The Platform shall consider items placed on its agenda by its chairman, either on his own initiative or at the request of on or more of its members.

Article 10
Amendment of Directive 2002/58/EC

Article 15 of Directive 2002/58/EC is amended as follows:

1. a new paragraph 2 is inserted which reads: "Paragraph 1 is not applicable to obligations relating to the retention of data for the prevention, investigation, detection and prosecution of criminal offences, as harmonised by Directive 2005/../EC.";

2. paragraphs 2 and 3 are renumbered to paragraphs 3 and 4.

Article 11
Evaluation

1. Not later than three years from the date referred to in Article 11(1), the Commission shall submit to the European Parliament and the Council an evaluation of the application of this Directive and its impact on economic operators and consumers, in particular taking into account the statistical elements provided to the Commission pursuant to article 7 of this Directive as to determine the necessity to modify the retention period referred to in article 5 of this Directive.

2. To this end, the Commission shall take into account any observations that might be communicated to it by Member States, by the Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC, or by the Platform set up under Article 9 of this Directive.

Article 12
Transposition

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by no later than 15 months after its adoption at the latest. They shall forthwith communicate to the Commission the text of those provisions and a correlation table between those provisions and this Directive.

   When Member States adopt those provisions, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.

2. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

Article 13
Entry into force

This Directive shall enter into force on the day of its publication in the *Official Journal of the European Union.*

Article 14
Addressees

This Directive is addressed to the Member States.

Done at Brussels, [...]

For the European Parliament	*For the Council*
The President	*The President*
[...]	[...]

Annex

Types of data to be retained under the categories identified in Article 4 of this Directive:

a) Data necessary to trace and identify the source of a communication:

(1) Concerning Fixed Network Telephony:

(a) The calling telephone number;

(b) Name and address of the subscriber or registered user;

(2) Concerning Mobile Telephony:

(a) The calling telephone number;

(b) Name and Address of the subscriber or registered user;

(3) Concerning Internet Access and Internet Communication Services:

(a) The Internet Protocol (IP) address, whether dynamic or static, allocated by the Internet access provider to a communication;

(b) The User ID of the source of a communication;

(c) The Connection Label or telephone number allocated to any communication entering the public telephone network;

(d) Name and address of the subscriber or registered user to whom the IP address, Connection Label or User ID was allocated at the time of the communication.

b) Data necessary to trace and identify the destination of a communication:

(1) Concerning Fixed Network Telephony:

(a) The called telephone number or numbers;

(b) Name(s) and address(es) of the subscriber(s) or registered user(s);

(2) Concerning Mobile Telephony:

(a) The called telephone number or numbers;

(b) Name(s) and address(es) of the subscriber(s) or registered user(s);

(3) Concerning Internet Access and Internet Communication Services:

(a) The Connection Label or User ID of the intended recipient(s) of a communication;

(b) Name(s) and address(es) of the subscriber(s) or registered user(s) of the intended recipient(s) of the communication.

c) Data necessary to identify the date, time and duration of a communication;

(1) Concerning Fixed Network Telephony and Mobile Telephony:

(a) The date and time of the start and end of the communication.

(2) Concerning Internet Access and Internet Communication Services:

(a) The date and time of the log-in and log-off of the Internet sessions based on a certain time zone.

d) Data necessary to identify the type of communication;

(1) Concerning Fixed Network Telephony:

(a) The telephone service used, e.g. voice, conference call, Short Message Service, Enhanced Media Service or Multi-Media Service.

(2) Concerning Mobile Telephony:

(a) The telephone service used, e.g. voice, conference call, Short Message Service, Enhanced Media Service or Multi-Media Service.

e) Data necessary to identify the communication device or what purports to be the communication device:

(1) Concerning Mobile Telephony:

(a) The International Mobile Subscriber Identity (IMSI) of the calling and called party;

(b) The International Mobile Equipment Identity (IMEI) of the calling and called party.

(2) Concerning Internet Access and Internet Services:

(a) The calling telephone number for dial-up access;

(b) The asymmetric subscriber line (ADSL) or other end point of the originator of the communication;

(c) The media access control (MAC) address or other machine identifier of the originator of the communication.

f) Data necessary to identify the location of mobile communication equipment:

(1) The location label (Cell ID) at the start and end of the communication;

(2) Location labels (Cell ID) throughout the communication;

(3) Data mapping between Cell IDs and their geographical location at the time of the communication.